CISEC

AISAC — AI Security Automation Center

Términos de Uso del Análisis de Seguridad

Programa de Prueba de Concepto (POC) — Comunidad Lanzadera

Versión	1.0
Fecha de emisión	Abril 2026
Ámbito de aplicación	POC Lanzadera — Uso exclusivo residentes
Clasificación	Confidencial — No distribuir
Contacto	info@cisec.es

> ⚠ **AVISO LEGAL IMPORTANTE**
>
> El uso de esta herramienta contra sistemas sin autorización expresa del propietario constituye un delito informático tipificado en el artículo 197 bis del Código Penal español. Lea este documento completo antes de proceder al análisis.

1. Introducción y Objeto

El presente documento establece los Términos de Uso aplicables al análisis de seguridad automatizado proporcionado por Consultoría de Inteligencia y Securización, S.L. (en adelante, CISEC) a través de la plataforma AISAC, en el marco del programa de Prueba de Concepto (POC) habilitado para los miembros de la comunidad Lanzadera.

Mediante el uso de esta herramienta, el usuario (en adelante, el Usuario) acepta íntegra e incondicionalmente los presentes Términos. Si el Usuario no está de acuerdo con alguna de las condiciones establecidas, deberá abstenerse de utilizar el servicio.

> **Ámbito de aplicación**
>
> Este servicio está disponible exclusivamente para empresas residentes en el ecosistema Lanzadera durante el período de POC definido por CISEC.
> El acceso a esta herramienta no genera ninguna relación contractual remunerada entre el Usuario y CISEC.

2. Datos Identificativos del Prestador

Denominación social	Consultoría de Inteligencia y Securización, S.L.
NIF / CIF	B24850877
Domicilio social	Calle Dublín 33C, 28232 Las Rozas de Madrid, Madrid
Correo de contacto	info@cisec.es
Sitio web	cisec.es · aisac.tech
Actividad	Servicios de ciberseguridad — Pentesting como Servicio (PTaaS)

3. Definiciones

A los efectos del presente documento, se entenderá por:

- Agente AISAC: El sistema de inteligencia artificial automatizado desarrollado por CISEC que realiza análisis de seguridad en modo pasivo sobre los sistemas indicados por el Usuario.
- Análisis en modo pasivo: Técnicas de reconocimiento de seguridad no intrusivas que incluyen resolución DNS, escaneo de puertos, fingerprinting de servicios, análisis de cabeceras HTTP/HTTPS, revisión de certificados TLS y correlación de vulnerabilidades conocidas (CVEs) por versión de software. Excluye expresamente la explotación activa de vulnerabilidades, envío de payloads maliciosos, fuerza bruta de credenciales y cualquier técnica que pueda causar interrupción de servicio.
- Sistema Analizado: El hostname, dominio o dirección IP introducida por el Usuario como objetivo del análisis.
- Informe de Seguridad: El documento generado por el Agente AISAC que recoge los resultados del análisis, enviado al correo electrónico indicado por el Usuario.
- Usuario: La persona física que, en representación de una empresa del ecosistema Lanzadera, accede y utiliza la herramienta POC de AISAC.

4. Declaración de Titularidad y Autorización — Condición Esencial

> ⚠ **AVISO LEGAL IMPORTANTE**
>
> Esta cláusula es la más importante del presente documento. Su incumplimiento puede tener consecuencias penales graves para el Usuario.

Al introducir un hostname, dominio o dirección IP en el formulario de análisis y aceptar los presentes Términos, el Usuario DECLARA EXPRESAMENTE Y BAJO SU EXCLUSIVA RESPONSABILIDAD que:

1. Es el propietario legítimo del Sistema Analizado o el administrador técnico autorizado del mismo.
2. En caso de no ser el propietario, dispone de autorización expresa, escrita y vigente del propietario del sistema para realizar el análisis de seguridad.
3. El Sistema Analizado es un sistema propiedad de la empresa que representa, un entorno de desarrollo, staging o pruebas bajo su control, o un sistema de tercero para el que ha obtenido las autorizaciones necesarias.

4. Comprende que la realización de análisis de seguridad sobre sistemas de terceros sin su consentimiento constituye un delito tipificado en el artículo 197 bis del Código Penal español, con penas de prisión de seis meses a dos años.

Registro de auditoría

CISEC registrará automáticamente el Sistema Analizado, la dirección IP desde la que se realiza la solicitud, el correo electrónico y los datos identificativos del Usuario, junto con el timestamp exacto de la solicitud.

Este registro constituirá el trazado de responsabilidad completo en caso de cualquier incidencia o reclamación.

5. Naturaleza y Alcance del Análisis

5.1 Qué hace el Agente AISAC

- Resolución y análisis DNS (registros A, AAAA, MX, TXT, NS, CNAME, SOA)
- Enumeración de subdominios mediante herramientas pasivas y consulta de logs de Certificate Transparency (crt.sh)
- Consultas al archivo histórico Wayback Machine para identificar recursos y endpoints expuestos previamente
- Consultas de registro WHOIS para identificación de titularidad y datos de registro del dominio
- Recolección pasiva de correos electrónicos y hostnames expuestos públicamente (theHarvester)
- Consultas a la API de Shodan para obtener información de servicios expuestos indexados públicamente (reconocimiento de red pasivo)
- Mapeo de red ASN/BGP para identificar el rango de IPs asociado a la organización (reconocimiento de red pasivo)
- Descubrimiento de parámetros de URL a partir de archivos y fuentes públicas indexadas (paramspider)
- Escaneo de puertos abiertos y fingerprinting de servicios
- Análisis de cabeceras HTTP/HTTPS y políticas de seguridad (CSP, HSTS, X-Frame-Options)
- Inspección de certificados TLS/SSL (validez, cadena de confianza, algoritmos)
- Correlación de versiones de software detectadas con CVEs públicos conocidos
- Detección de tecnologías y frameworks expuestos
- Análisis de configuraciones de seguridad básicas (DMARC, DKIM, SPF)

5.2 Qué NO hace el Agente AISAC

- No ejecuta exploits ni payloads maliciosos contra el sistema
- No realiza ataques de fuerza bruta sobre credenciales o formularios
- No accede ni modifica datos almacenados en el sistema
- No realiza inyecciones SQL, XSS u otras técnicas de explotación activa
- No genera tráfico agresivo que pueda causar denegación de servicio
- No pivota hacia sistemas de red internos accesibles desde el host analizado

Nota técnica importante

El agente aplica rate limiting automático para no generar carga significativa en el sistema analizado.
Sin embargo, algunos sistemas con alertas de seguridad muy sensibles pueden registrar las conexiones del agente como actividad sospechosa. Esto es normal y esperado en un análisis de seguridad legítimo.
Si el sistema analizado genera alertas de seguridad como consecuencia del análisis autorizado, CISEC no tiene responsabilidad sobre las acciones de respuesta que los sistemas automáticos del Usuario puedan tomar.

6. Restricciones de Uso

El Usuario se compromete expresamente a NO utilizar el Agente AISAC para:

- Analizar sistemas de terceros sin disponer de autorización escrita de su propietario
- Introducir direcciones IP pertenecientes a rangos privados RFC 1918 (10.x.x.x, 172.16-31.x.x, 192.168.x.x) salvo sistemas bajo su control en dichos rangos
- Analizar infraestructuras críticas (hospitales, utilities, administraciones públicas) sin las autorizaciones correspondientes
- Eludir controles de seguridad o intentar acceder a funcionalidades no previstas en el POC
- Utilizar los resultados del Informe de Seguridad para actividades ilícitas o para facilitar ataques a terceros
- Compartir credenciales de acceso al POC con personas ajenas a la empresa representada

CISEC se reserva el derecho de suspender el acceso al POC de forma inmediata y sin previo aviso en caso de detectar un uso contrario a los presentes Términos, reservándose el derecho de ejercer las acciones legales que correspondan.

7. Limitación de Responsabilidad de CISEC

7.1 Exoneración por uso indebido

CISEC queda expresamente exonerada de toda responsabilidad derivada de:

- La introducción por parte del Usuario de sistemas que no le pertenecen o para los que no dispone de autorización
- Interrupciones, alertas de seguridad o efectos secundarios del análisis sobre sistemas correctamente autorizados por el Usuario
- Decisiones técnicas o de negocio adoptadas por el Usuario en base al Informe de Seguridad
- La exactitud, completitud o vigencia de la información de vulnerabilidades incluida en el Informe, que se proporciona con fines informativos y sin carácter exhaustivo

7.2 Limitación general de responsabilidad

En ningún caso la responsabilidad total de CISEC frente al Usuario derivada del uso del POC superará la cantidad de cero euros (0 €), al tratarse de un servicio gratuito en el marco del programa de validación comercial. Lo anterior no limita la responsabilidad de CISEC en los casos en que la ley aplicable no permita tal limitación.

7.3 Disponibilidad del servicio

El POC se proporciona "tal cual" (as-is) sin garantías de disponibilidad, tiempo de respuesta o exactitud de resultados. CISEC no asume ningún compromiso de nivel de servicio (SLA) en el marco del presente POC.

8. Protección de Datos Personales

El tratamiento de los datos personales del Usuario en el marco de este POC se rige por el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD).

8.1 Datos recogidos y finalidad

Dato	Finalidad	Retención
Nombre y empresa	Identificación y trazabilidad de auditoría	12 meses
Correo electrónico	Envío del Informe de Seguridad	12 meses
Hostname / IP analizado	Registro de scope autorizado (auditoría legal)	2 años
IP de origen de la solicitud	Prevención de fraude y trazabilidad de auditoría	2 años
Timestamp de solicitud	Registro de auditoría	2 años

8.2 Base legal y derechos del interesado

La base legal del tratamiento es el interés legítimo de CISEC en la prevención de usos fraudulentos de la herramienta (art. 6.1.f RGPD) y la ejecución de las condiciones de uso aceptadas por el Usuario (art. 6.1.b RGPD).

El Usuario puede ejercer sus derechos de acceso, rectificación, supresión, portabilidad y oposición dirigiéndose a info@cisec.es con el asunto 'Ejercicio de Derechos RGPD — POC Lanzadera'. CISEC responderá en el plazo de un mes. El Usuario también puede presentar una reclamación ante la Agencia Española de Protección de Datos (aepd.es).

El Informe de Seguridad generado puede contener información técnica sensible sobre los sistemas del Usuario. CISEC no compartirá este informe con terceros y lo tratará como información confidencial. Los datos del análisis podrán utilizarse de forma anonimizada para mejorar los modelos de detección de AISAC.

9. Confidencialidad del Informe

El Informe de Seguridad generado por el Agente AISAC contiene información técnica sensible sobre la infraestructura del Usuario y debe ser tratado como documento confidencial.

- El Usuario no debe compartir el Informe con terceros no autorizados
- El Informe se envía únicamente al correo electrónico indicado por el Usuario en el formulario
- El Informe no debe publicarse íntegramente en canales públicos sin anonimizar los datos técnicos
- CISEC podrá conservar una copia del Informe durante el período de retención indicado en la cláusula 8 únicamente con fines de auditoría interna

10. Propiedad Intelectual

El Agente AISAC, su metodología de análisis, los algoritmos de correlación, el formato del Informe de Seguridad y todos los elementos que componen la plataforma son propiedad exclusiva de CISEC y están protegidos por la normativa de propiedad intelectual e industrial vigente.

El uso del POC no otorga al Usuario ningún derecho de licencia, sublicencia, distribución o reproducción sobre ningún componente de la plataforma AISAC.

Los resultados del análisis contenidos en el Informe de Seguridad son propiedad del Usuario en lo que respecta a la información técnica de sus propios sistemas.

11. Legislación Aplicable y Jurisdicción

Los presentes Términos se rigen por la legislación española, en particular:

- Reglamento (UE) 2016/679 relativo a la protección de datos personales (RGPD)
- Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)
- Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE)
- Ley Orgánica 10/1995 del Código Penal, especialmente el artículo 197 bis relativo a accesos informáticos no autorizados
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual

Para la resolución de cualquier controversia derivada de los presentes Términos, las partes se someten, con renuncia expresa a cualquier otro fuero que pudiera corresponderles, a los Juzgados y Tribunales de Madrid capital.

12. Modificaciones y Vigencia

CISEC se reserva el derecho de modificar los presentes Términos en cualquier momento durante el período de vigencia del POC. Las modificaciones serán comunicadas a los Usuarios con un preaviso mínimo de 7 días naturales mediante correo electrónico a la dirección registrada. El uso continuado de la herramienta tras la comunicación de los cambios implica la aceptación de los nuevos Términos.

Los presentes Términos entran en vigor en el momento de su aceptación por el Usuario a través del mecanismo habilitado en el formulario de análisis y permanecerán vigentes durante todo el período del POC Lanzadera o hasta que CISEC proceda a su revocación o sustitución.

13. Aceptación

Declaración de aceptación expresa e informada

Al marcar la casilla de aceptación en el formulario de análisis, el Usuario confirma que:

(a) Ha leído y comprendido íntegramente los presentes Términos de Uso.
(b) Acepta de forma libre, voluntaria e informada todas las condiciones establecidas.
(c) Declara ser propietario o administrador autorizado del sistema que introduce.
(d) Comprende las implicaciones legales del análisis de sistemas sin autorización.

Esta aceptación tiene la misma validez jurídica que una firma manuscrita conforme a la Ley 34/2002 (LSSI-CE) y el Reglamento (UE) 910/2014 sobre identificación electrónica (eIDAS).

Consultoría de Inteligencia y Securización, S.L. — CISEC
Calle Dublín 33C, 28232 Las Rozas de Madrid · info@cisec.es · cisec.es · aisac.tech
Versión 1.0 — Abril 2026 — Documento confidencial. No distribuir sin autorización de CISEC.

